Intel® Solid-State Drive Professional 1500 Series and Secure Erase

White Paper

May 2014

Revision 1.0

NFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Solid-State Drives may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

Intel does not control or audit the design or implementation of third party benchmark data or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmark data are reported and confirm whether the referenced benchmark data are accurate and reflect performance of systems available for purchase.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2014 Intel Corporation. All rights reserved.

Protecting Confidential Corporate Data while Repurposing or Retiring PCs

Why Secure Erase?

Solid-State Drives (SSDs) are increasingly used in mobile PCs, delivering significant performance boosts and enhanced physical durability unheard of a decade ago when Hard Disk Drives (HDDs) were popular. We are no longer dependent on HDDs slower and less reliable spinning magnetic media. SSDs are truly a game-changing technology.

Investing in new, improved technologies is imperative for corporations and individuals committed to keeping pace with ever-evolving business demands. In an effort to remain on the cutting edge, businesses periodically replace and upgrade their PCs. Existing PCs are often repurposed for new employees. Consumers upgrade to larger capacity storage devices when their drive reaches capacity, or when the price of larger drives drop to a more cost-efficient level. However, leaving data on repurposed drives is a significant concern. SSDs have changed the way we think about data remaining on the drive after the drive has been retired.

Removing information from any storage device can be challenging. Using the operating system based “delete” file or folder doesn’t permanently erase stored data. Even a “format drive” does not completely erase data. Data retention is typically desirable, but not after the user believed that the data had been erased. Well-funded and malicious individuals use advanced techniques to probe the storage areas of drives to extract information. The need for an effective way to remove data, and then verify that it cannot be retrieved, is fundamental to supporting data confidentiality–the motivation behind Secure Erase. This whitepaper explains the Secure Erase process and describes how Secure Erase helps to protect confidential data.

What is Secure Erase?

Secure Erase is a data erase method supported by the drive’s controller which removes stored data from the drive’s memory. Secure Erase is an irreversible process. Once a Secure Erase is performed on a drive, its content is unrecoverable. Secure Erase is initiated through a standard ATA command to a drive’s controller by means of the drive’s IO interface and overwrites the NAND blocks on the drive (in-use and spare) with zeros and generates a new Media Encryption Key (MEK).

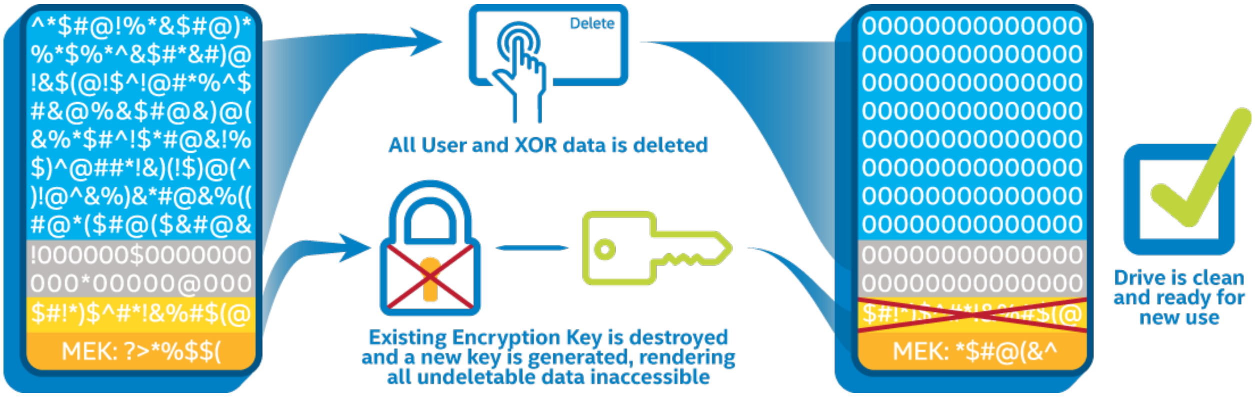
Secure Erase is supported on all Intel SSD Professional Family products, including the Intel® Solid-State Drive Professional 1500 Series. All Intel SSD Professional Family drives are self-encrypting. These self-encrypting drives use a unique MEK to cryptographically encode/decode data stored on the SSD. The encryption is done automatically by the SSDs on-board controller and is done in real-time, so the data transfer rate is not impacted. By directing the SSDs controller to generate a new MEK, subsequent reads from the drive remain encrypted and unintelligible.

Intel's Secure Erase Process

When issuing a Secure Erase command on an Intel® SSD Pro 1500 Series product, the goal is to remove all existing user data from the storage media. No user information can be read from the NAND memory chips after performing the Secure Erase.

Two steps are necessary to accomplish the goal of removing data. The first step in removing data is to overwrite all data storage locations in the memory with a "0". This write operation permanently removes previously stored data on NAND chips. A single write is effective on NAND memory. Magnetic storage media used on HDDs requires multiple writes to remove any data artifacts.

The second step to securely removing data is to generate a new MEK, making any data on the SSD undecipherable. This extra step makes unused memory locations unreadable. NAND memory can wear out over time, typically after several million writes. Generating a new MEK is important because one of the Intel SSD Pro 1500 Series capabilities is to replace memory that wears out over time with good spare memory, similar to a spare tire. The worn out, replaced NAND memory blocks are no longer used, but may contain old user data. It is important to erase this data, but often the worn out NAND can't be overwritten. The old data on the worn out blocks cannot be read without the original MEK, unless extraordinary and time consuming measures are used. Generating a new MEK keeps any SSD data location, active or spare, unreadable since it was encrypted with the old MEK.



National Institute of Standards and Technology* Approval

Protecting confidential information on previously used SSDs is an important issue for IT administrators, especially if the drive will be reused or leave the corporate environment. The Intel Pro 1500 Series Secure Erase feature was designed to remove data in a secure way, eliminating the ability for data reconstruction. The National Institute of Standards and Technology* (NIST), a US government agency overseeing security methods, considers Secure Erase the best method to delete the contents of an SSD.

NIST published a *Special Publication 800-88, Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology* (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf), establishing a standard for purging data from data storage devices. NIST rates the Secure Erase method higher than software overwriting or any "clear" technology. In fact, Secure Erase is the highest level of security short of physically destroying the drive. The Intel® SSD Pro 1500 Series meets the strict NIST guidelines.

Intel's implementation of Secure Erase purges all existing data and generates a new MEK to help render even retired blocks of memory unreadable. In an effort to validate the effectiveness of the Secure Erase feature offered on its SSD Pro 1500 Series, Intel contracted with Kroll OnTrack Inc.*, a leading storage device testing company. Kroll independently tested multiple Intel SSDs to verify that all usable data was removed from the device and no remnant data was accessible. After rigorous analysis, Kroll confirmed the Secure Erase process deployed by Intel accomplished these goals.

Intel's IT Group Uses Secure Erase

Intel's IT department was an early adopter of SSDs for employees and has deployed Intel SSDs to over 100,000 employees. One of the key challenges for Intel IT was the retiring or redeployment of Intel SSDs during the PC refresh cycle due to Intel's strict reuse policies designed to protect its intellectual property and employee's personal information. The Intel IT department determined that the use of Secure Erase would be central to meeting these policies.

Intel's published whitepaper, *The Full Mobile Deployment Benefits of Intel's Solid State Drives* (http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/full-mobile-deployment-benefits-of-Intel-ssds-paper.pdf), explains the philosophy and solutions used to manage SSDs within their diverse worldwide environment. The whitepaper highlights Intel's support of SSDs and Secure Erase.

Using Secure Erase with the Intel® SSD Pro 1500 Series

Intel's SSD Toolbox supports the Secure Erase feature. This Windows*-based tool is available on the Intel web site (www.intel.com/go/ssdtoolbox) and can be used to issue a Secure Erase to an Intel SSD Pro 1500 Series drive secondarily connected to a PC (by means of, a drive other than the C: drive).

Other tools may be able to issue a Secure Erase command. The Secure Erase command can only be issued by a well-defined "Security Provider" in the form of a third-party software application, and not from within the operating system (OS) environment. Prior to the OS boot, the system BIOS issues a Secure Lock command preventing alteration by other system agents.

Secure Erase and Opal

The Intel SSD Pro 1500 Series supports the Trust Computing Group's* (TCG) Opal security standard. Opal is the drive's authentication method which allows access to the drive's contents, including the operating system files, to authorized users. If Opal is activated on an Intel SSD Pro 1500 Series, a password is required to change the drive's configuration or to access the drive's contents. An Opal-activated Intel SSD Pro 1500 Series will perform a Secure Erase command only after the authorized user deactivates Opal. This security feature prevents an unauthorized agent from maliciously erasing an SSD.

A Secure Erase You Can Trust

Protecting your company's data is crucial. Your SSD should not compromise security during active use, or after it has been repurposed. The Intel SSD Pro 1500 Series supports an industry-approved Secure Erase method, validated by independent testing. You can feel confident using Intel's Professional Family SSDs to store your confidential information, and to keep that information confidential, by using our Secure Erase feature.